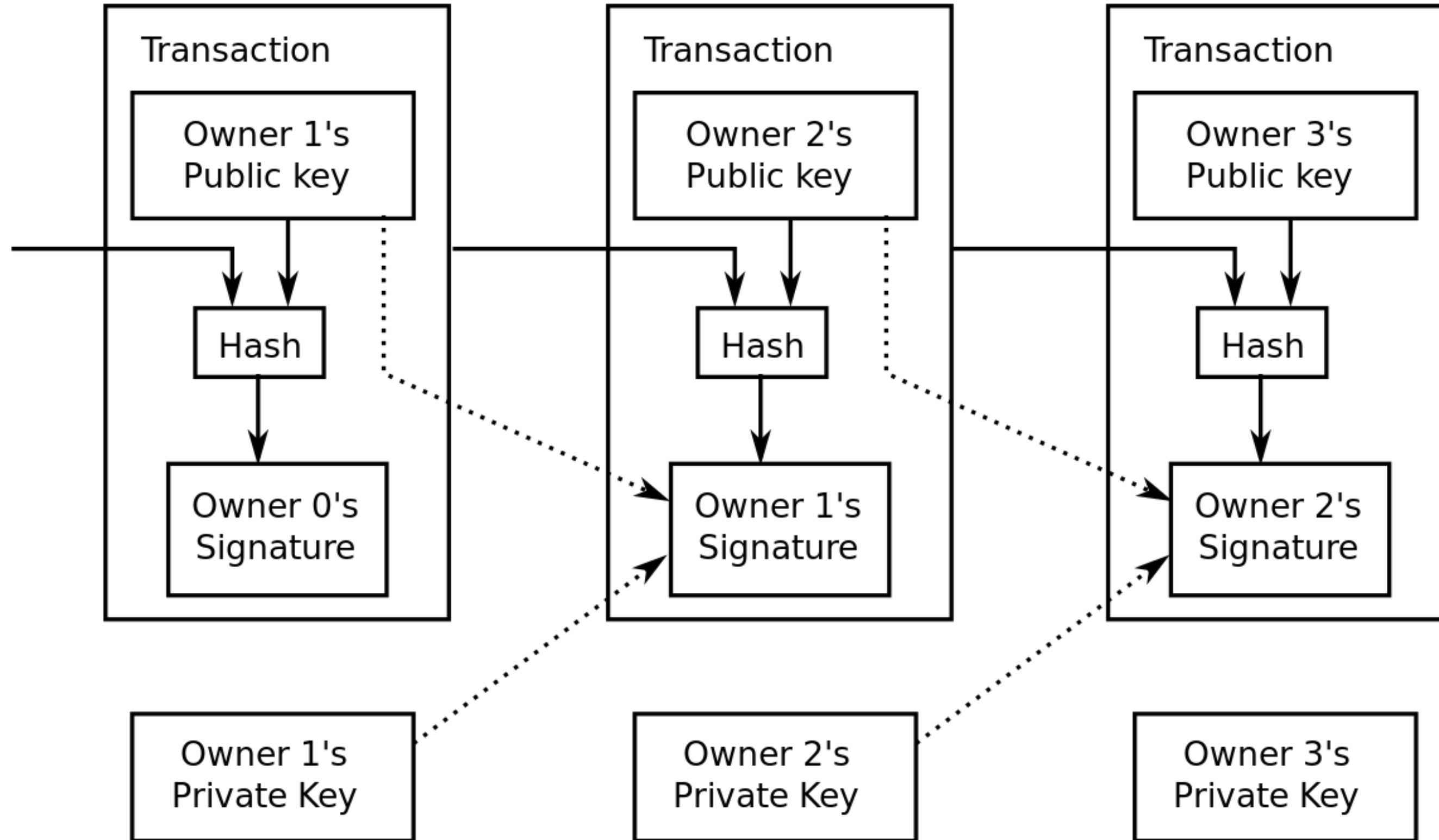


Mercury layer

A private non-custodial layer-2 for Bitcoin

Tom Trevethan - CTO Commerceblock

Bitcoin transactions



Transactions change ownership

Require confirmation in
blockchain

Limited space: high fees and
long confirmation times

Private keys ...

Can we just send private keys?

Owner 1



Owner 2



Off-chain: free, instant and private

BUT: have to trust sender to delete their key

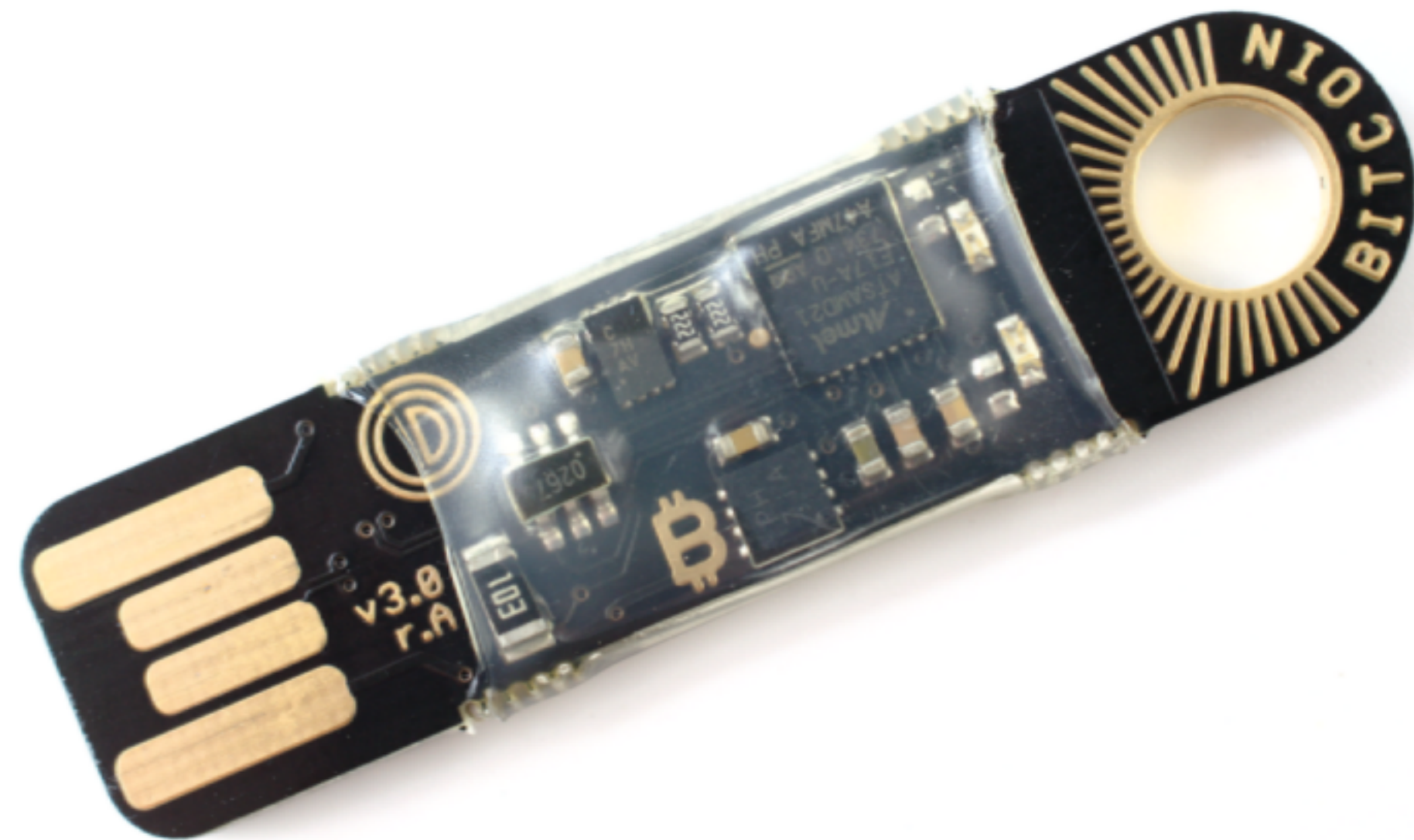


Private keys ...

How to prevent the previous owner from stealing?

1. Via trusted hardware

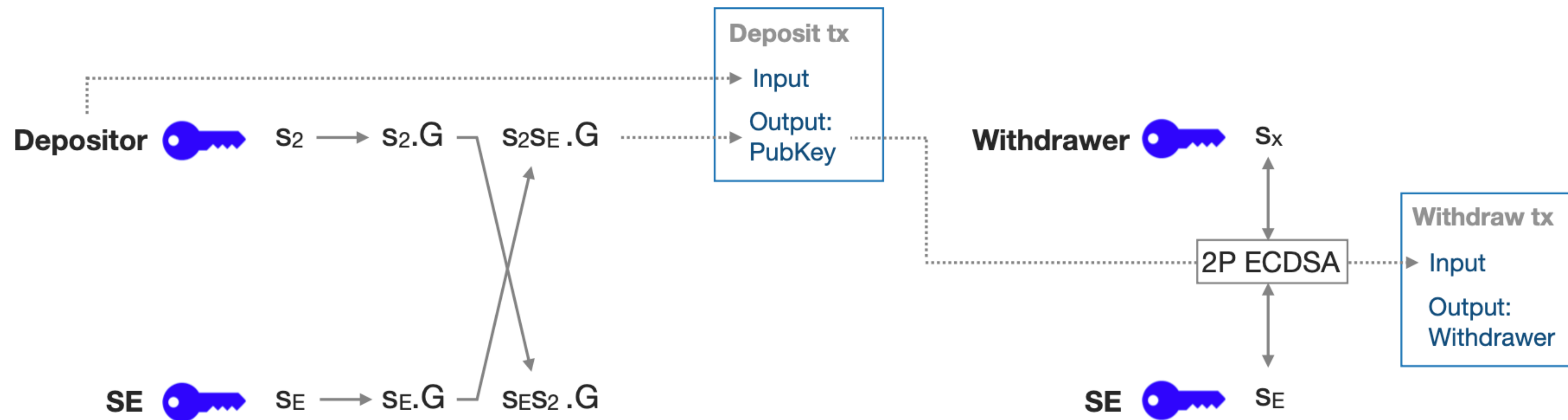
e.g. **Opendime**



Private keys ...

How to prevent the previous owner from stealing?

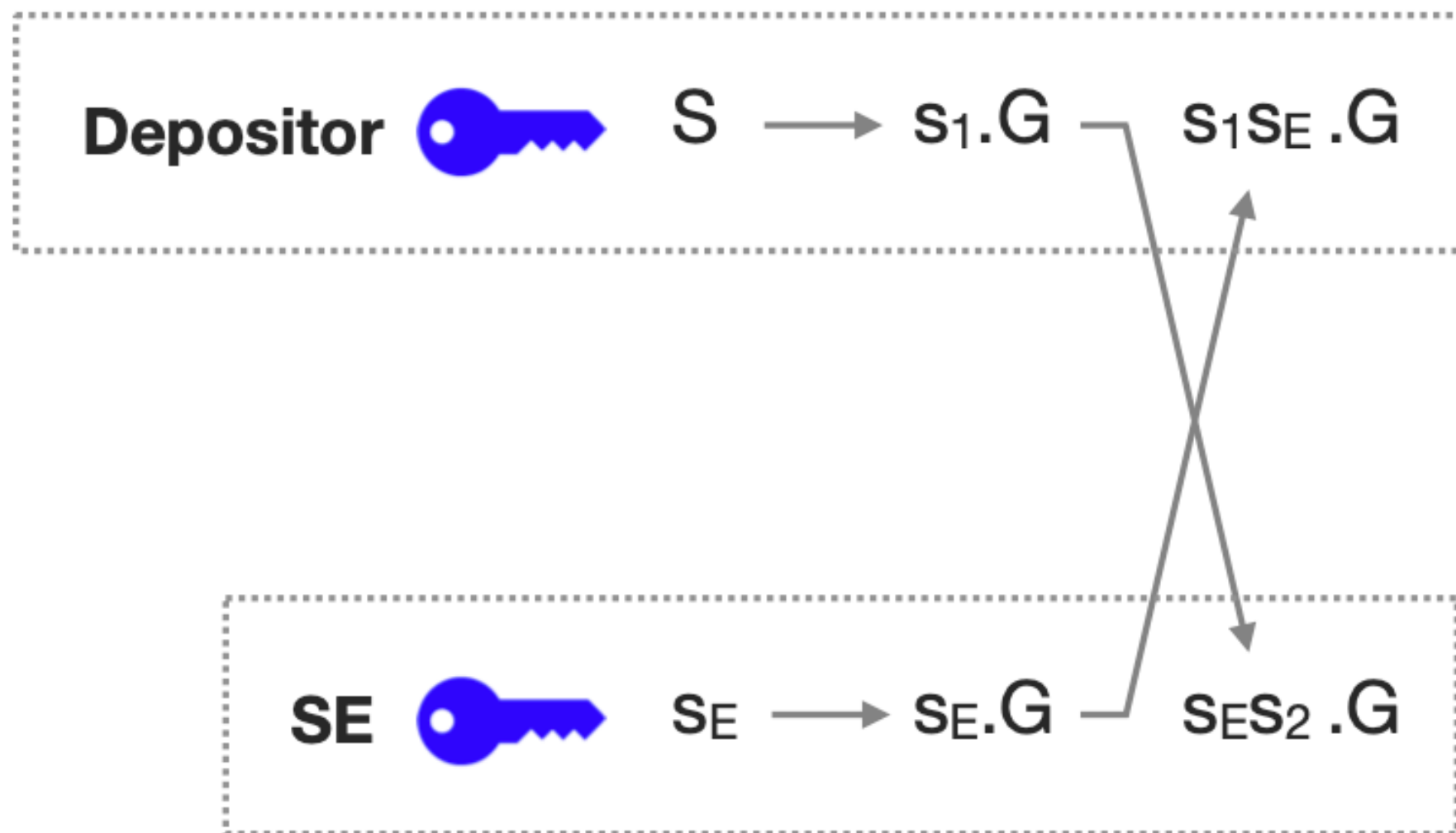
2. Using a trusted *key-share update server*: **Statechains**



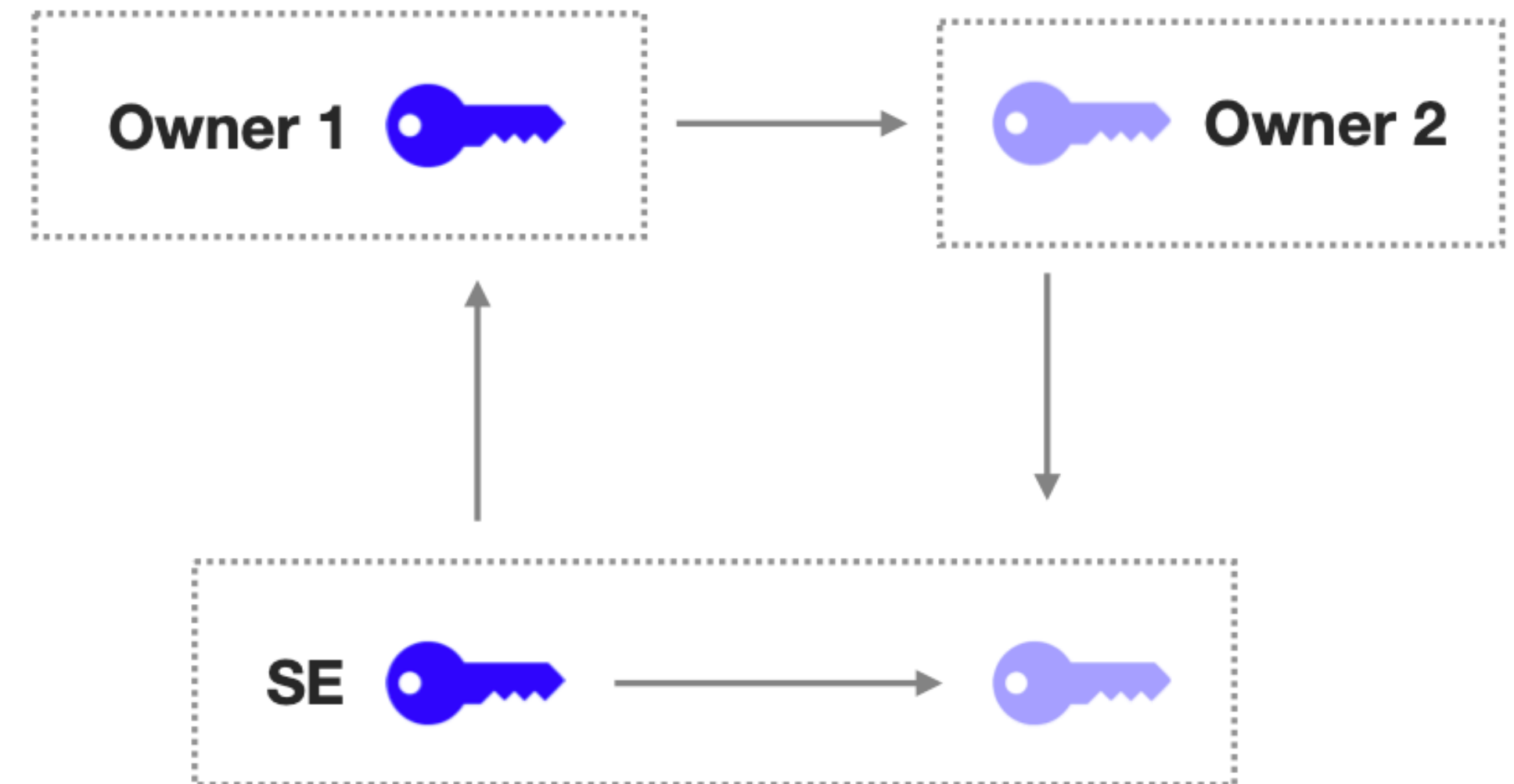
Mercury protocol

Single shared public key → P2(W)PKH on-chain output

Multiplicative private shares: $\mathbf{P} = s_1 s_E .G$. (shared secret key $s_1 s_E$ is never computed or known)



Transfer: Key share update protocol

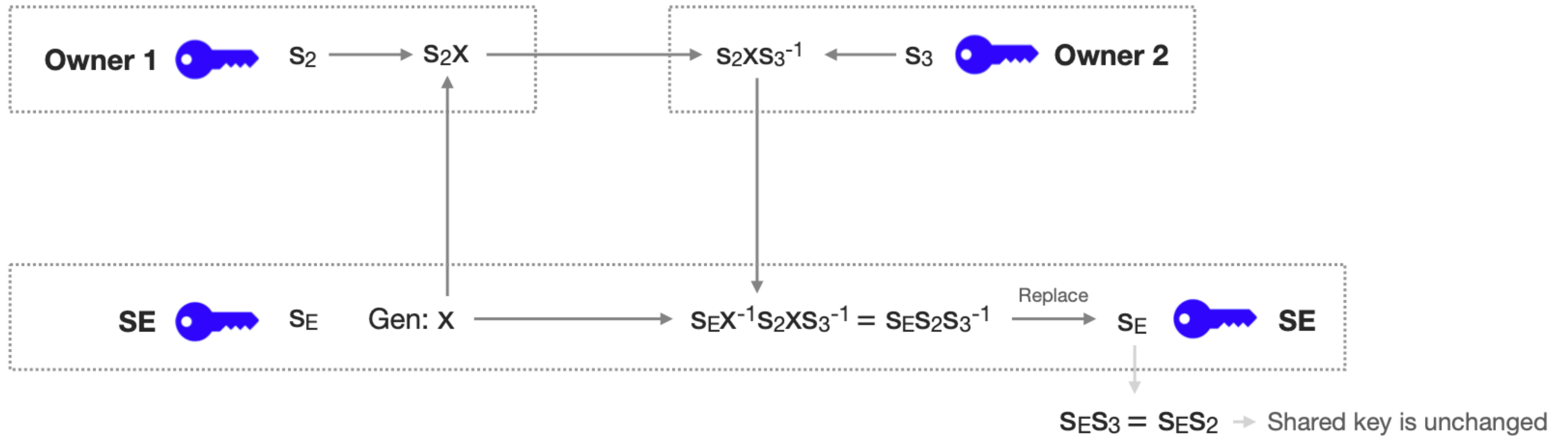


If the previous value of s_E is deleted, previous owners cannot steal the UTXO even if s_E colludes or is hacked.

Mercury protocol

Transfer: Key share update protocol

Multiplicative private shares: **PubKey** = $s_1s_1.G$. (shared secret key s_1s_1 is never computed or known)



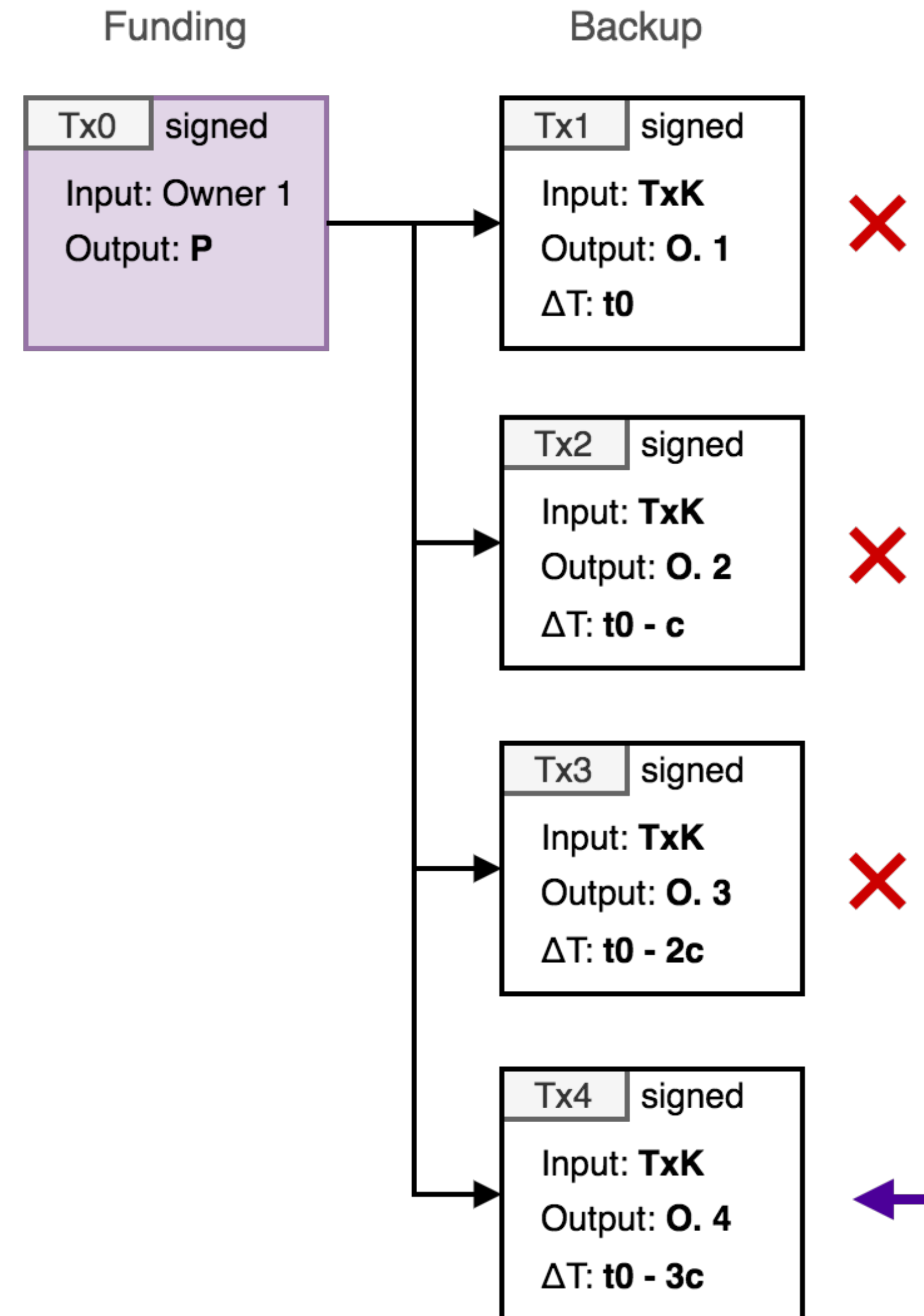
→ *Proactively non-custodial*

Mercury protocol

Off-chain (backup) transactions via **decrementing nLocktime**

- Compatible with current Bitcoin protocol rules
- Previous owner attacks not possible

... this limits number of transfers and statecoin lifetime



Mercury wallet

Launched 2021:

Over 25 BTC deposited

Over 80,000 coin swaps

But:

- Public keys and TxIDs known to server
- Statecoin UTXOs identifiable on-chain
- 2-Party ECDSA complex and slow

The screenshot displays the Mercury wallet interface. At the top, the logo 'mercury wallet' is on the left, and 'TOR / I2P' with a toggle switch, a help icon, a settings gear, and a share icon are on the right. The main balance section shows '0.653 BTC' with a padlock icon and '6 Statecoins in Wallet'. Below this is a 'Hide balance' toggle switch. Action buttons include 'DEPOSIT' (orange), 'WITHDRAW' (orange), 'SWAP' (blue), 'SEND' (blue), and 'RECEIVE' (blue). A status bar below shows 'Connected to Server' (green), 'Connecting to Swaps' (grey), and 'Connected to Bitcoin' (green). The 'ACTIVITY' tab is selected, showing a list of statecoin transactions. The first entry is '0.5 BTC' (grey icon), 'Original', with a progress bar and 'Time Until Expiry' indicator, and 'Phase 7/8: finalizing transfers'. The second entry is '0.1 BTC' (orange icon), 'Swaps: 148', with a progress bar, 'Time Until Expiry' indicator, and 'Expired' status. The third entry is '0.05 BTC' (orange icon), 'Swaps: 142', with a progress bar, 'Time Until Expiry' indicator, and 'Expired' status. The fourth entry is '0.001 BTC' (orange icon) with a progress bar and 'Time Until Expiry' indicator.

Mercury wallet

Launched 2021:

Over 25 BTC deposited

Over 80,000 coin swaps

But:

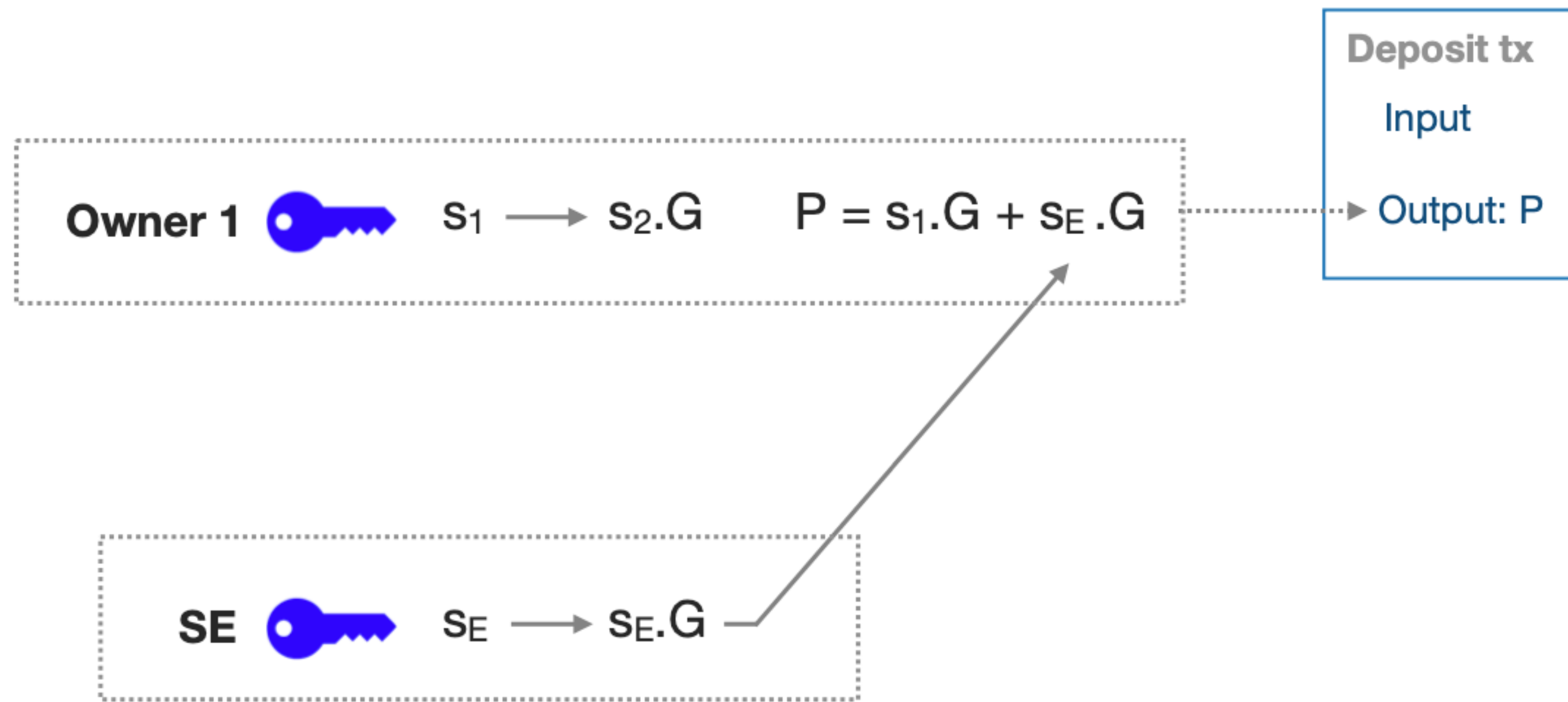
- Public keys and TxIDs known to server
- Statecoin UTXOs identifiable on-chain
- 2-Party ECDSA complex and slow

Solutions:

- Blind 2 party Schnorr signatures (MuSig)
- Statechain entity signature count
- Full client-side verification
Server only reports *number* of co-signings
- Server completely blind to any on-chain identification

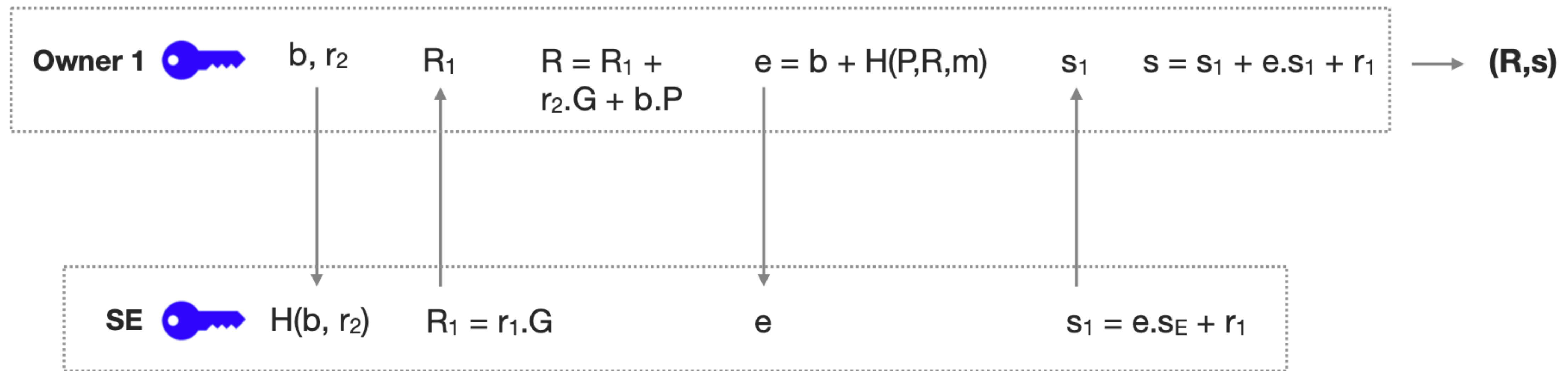
Blind 2-Party Schnorr

- Two parties required to generate a signature on shared public key
- One party (**SE**) does not learn: 1) The full shared public key. 2) The message (sighash) or 2) The final signature



Blind 2-Party Schnorr

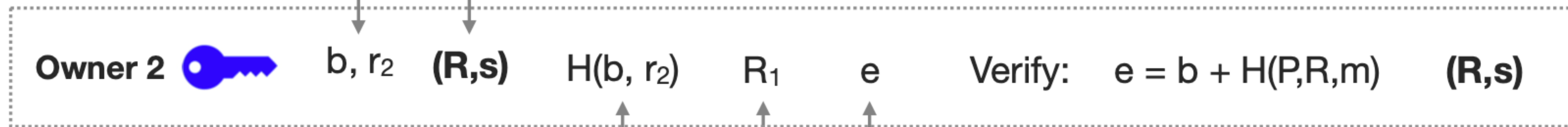
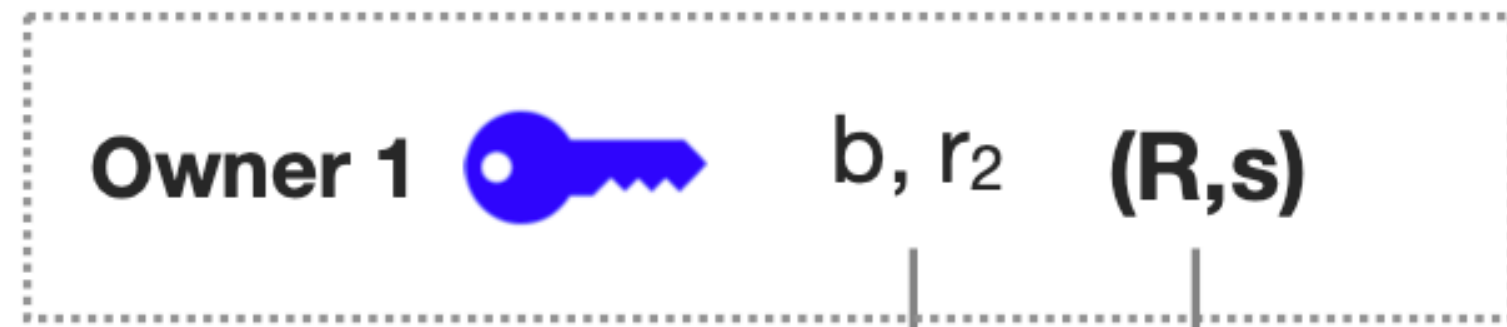
- Two parties required to generate a signature on shared public key
- One party (**SE**) does not learn: 1) The full shared public key. 2) The message (sighash) or 2) The final signature



Blind 2-Party Schnorr

New owner verifies all previous signatures co-generated with the SE

New owners verifies all previous backup txs (m) are time locked and valid



Commitment to (b, r_2) and verification of e prevents 'one-more-signature' and Wagner attacks against blinded Schnorr

Mercury Layer

Blind 2-party Schnorr enables a completely blind SE. SE trusted to report number of signatures, instead of enforcing rules.

SE is unable to have any knowledge of the on-chain identity of coins

Mercury Layer + atomic coinswaps completely on-chain transaction graph

Lightning latch protocol enables atomic statecoin/LN transactions

Blinded version of MuSig2 (with TC/HSM support)

Mercury layer server (Rust)

Mercury layer WASM (Rust) client

React-app client

github.com/commerceblock/mercurylayer

Telegram: mercurywallet



Bitcoin 2nd layers:

Lightning:

Trustless (in principle)
Verifiable
Unilateral exit
Requires liquidity
Arbitrary Payments (dependent on channels)

Mercury:

Trust required
Verifiable
Unilateral exit
Pro-actively non-custodial
Whole UTXOs
Completely blind

Fedimint/Cashu:

Trust required
Non-verifiable
Fully custodial
Arbitrary Payments
Private payments
Deposit/withdrawal identifiable

Liquid:

Trust required
Verifiable
Fully custodial
Arbitrary Payments
Peg in/out identifiable